Two-Factor Authentication and Policy

Category: Security & Logging In

DRAFT

This article is being reviewed for completeness and technical accuracy.

What is two-factor authentication?

In the field of security, there are three general ways you can prove you are who you claim to be. Each way is called a "factor." The factors fall into the categories of (1) something you have, such as an ATM card, (2) something you know, such as the personal pin to your bank account, and (3) something you are, such as your fingerprint. Two-factor authentication refers to using any two of these factors to authenticate a person before access to systems is granted.

NAS Policy

At NAS, the three different factors used are:

1. your assigned RSA SecurID fob (sometimes called a key fob or a token)
2. your password to the NAS systems
3. your public/private key pair

You are required to authenticate yourself with two of these factors before you can access NAS resources from outside the NAS HECC Enclave. One of these two factors has to be the possession of your SecurID fob. Thus, you can authenticate yourself with a combination of either SecurID + password, or SecurID + public/private key pair.

Two-factor authentication is required when accessing

- the secure front-end systems, SFE1 and SFE2, from your local desktop systems
- any system inside the NAS HECC Enclave (such as Pleiades or Columbia) from your localhost using SSH Pasthrough.
- Bouncer or Bruiser (bastion hosts to other NAS desktop systems) from your local desktop systems
- Return to Flight (RTF) hosts through the web

Related articles: RSA SecurID Fob, Passwords, Public/Private Key Pairs

Article ID: 32
Last updated: 04 Mar, 2011
The HEC Environment -> Security & Logging In -> Two-Factor Authentication and Policy
http://www.nas.nasa.gov/hecc/support/kb/entry/32/?ajax=1